DIALOG(R)File 351:Derwent WPI

011142335 **Image available**
WPI Acc No: 1997-120259/199712
XRPX Acc No: N97-098916
Microprocessor system for safety critical applications e.g. for motor vehicle ABS, ASR etc systems - has duplicated processor systems with outputs applied to comparators to control shut-down
Patent Assignee: ITT AUTOMOTIVE EURO GMBH (INTT); CONTINENTAL TEVES & CO OHG AG (TEVE); CONTINENTAL TEVES AG & CO OHG (TEVE); ITT MFG ENTERPRISES INC (INTT)
Inventor: GIERS B
Number of Countries: 020 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 19529434	A1	19970213	DE 1029434	A	19950810	199712 B
WO 9706487	A1	19970220	WO 96EP2688	A	19960620	199714
EP 843853	A1	19980527	EP 96922870	A	19960620	199825
			WO 96EP2688	A	19960620	
EP 843853	B1	19990901	EP 96922870	A	19960620	199940
			WO 96EP2688	A	19960620	
DE 59602962	G	19991007	DE 502962	A	19960620	199947
			EP 96922870	A	19960620	
			WO 96EP2688	A	19960620	
JP 11510925	W	19990921	WO 96EP2688	A	19960620	199950
			JP 97508049	A	19960620	
KR 99036222	A	19990525	WO 96EP2688	A	19960620	200032
			KR 98700890	A	19980206	
US 6201997	B1	20010313	WO 96EP2688	A	19960620	200120
			US 9811439	A	19980407	
KR 369492	B	20030410	WO 96EP2688	A	19960620	200353
			KR 98700890	A	19980206	

Priority Applications (No Type Date): DE 1029434 A 19950810
Cited Patents: 1.Jnl.Ref; DE 3234637; EP 306348; EP 372579; JP 7160521
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19529434	A1		6	G05B-009/03	
WO 9706487	A1	G	21	G06F-011/18	
	Designated States (National): JP KR US				
	Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE				
EP 843853	A1	G		G06F-011/18	Based on patent WO 9706487
	Designated States (Regional): DE FR GB				
EP 843853	B1	G		G06F-011/18	Based on patent WO 9706487
	Designated States (Regional): DE FR GB				
DE 59602962	G			G06F-011/18	Based on patent EP 843853
					Based on patent WO 9706487
JP 11510925	W		14	G06F-011/18	Based on patent WO 9706487
KR 99036222	A			G06F-011/18	Based on patent WO 9706487
US 6201997	B1			G05B-009/02	Based on patent WO 9706487
KR 369492	B			G06F-011/18	Previous Publ. patent KR 99036222
					Based on patent WO 9706487

Abstract (Basic): DE 19529434 A

The safety critical system employs duplicated microprocessor systems [MC1,MC2] that have processors [1,2] and operate on the same data and use the same programs. Each has read-only memories (ROM) [5,10 and write-read memories (RAM) [6,11]. The output of the processors is received by external comparators [18,19] and if the data is not in agreement shutdown is signalled. Each of the controllers has a separate bus system [3,4] coupled to drive stages [15-17].

USE/ADVANTAGE - Automotive systems. Provides protection against processing faults

Dwg.1/1

Title Terms: MICROPROCESSOR; SYSTEM; SAFETY; CRITICAL; APPLY; MOTOR; VEHICLE; SYSTEM; DUPLICATE; PROCESSOR; SYSTEM; OUTPUT; APPLY; COMPARATOR; CONTROL; SHUT; DOWN
Derwent Class: Q11; Q52; T01; T06; X22
International Patent Class (Main): G05B-009/02; G05B-009/03; G06F-011/18
International Patent Class (Additional): B60B-039/00; F02D-045/00; G05B-019/18; G06F-013/38; G06F-015/16; G06F-019/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-J07C; T06-A03; X22-C02C1; X22-C02C3
?

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Offenlegungsschrift

(10) DE 195 29 434 A1

(51) Int. Cl.[6]:
G 05 B 9/03
// B60T 8/60,8/88, B60K 28/16,G06F 11/18

(21) Aktenzeichen: 195 29 434.3
(22) Anmeldetag: 10. 8. 95
(43) Offenlegungstag: 13. 2. 97

DE 195 29 434 A1

(71) Anmelder:
ITT Automotive Europe GmbH, 60488 Frankfurt, DE

(72) Erfinder:
Giers, Bernhard, 64380 Roßdorf, DE

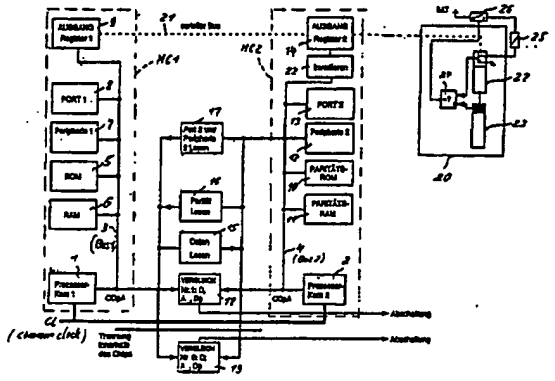
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 32 34 637 C2
DE 30 24 370 C3
DE 43 41 082 A1
DE 41 37 124 A1
DE 39 38 501 A1
DE 35 33 849 A1
DE 32 25 455 A1
EP 05 18 630 A2

NIX,H.G.: Sichere Mikroprozessorsysteme für Schutzaufgaben bei der Prozeßautomatisierung. In: Automatisierungstechnische Praxis atp, 28.Jg., 1986, H.3, S.130-135;

(54) Microprozessorsystem für sicherheitskritische Regelungen

(57) Ein Mikroprozessorsystem für sicherheitskritische Regelungen umfaßt zwei synchron betriebene Zentraleinheiten (1, 2), die die gleichen Eingangsdaten erhalten und das gleiche Programm abarbeiten, außerdem Festwertspeicher (5, 10) und Schreib-Lese-Speicher (6, 11) für Nutzdaten und Prüfdaten und außerdem Vergleicher (18, 19), die die Ausgangssignale der Zentraleinheiten (1, 2) überprüfen und bei Nicht-Übereinstimmung Abschaltsignale abgeben. Die Zentraleinheiten (1, 2) sind über separate Bussysteme (3, 4) an die Speicher sowie an die Eingabe- und Ausgabeeinheiten angeschlossen und durch Treiberstufen (15-17) gekoppelt, die den Zentraleinheiten (1, 2) ein gemeinsames Lesen und Abarbeiten der in beiden Bussystemen (3, 4) zur Verfügung stehenden Daten ermöglichen.



DE 195 29 434 A1

Beschreibung

Die Erfindung bezieht sich auf ein für sicherheitskritische Regelungssysteme v rgesehenes Micropr zessorsystem, das zwei synchron betriebene Zentraleinheiten oder CPU's enthält, die die gleichen Eingangsinformationen erhalten und das gleiche Programm abarbeiten, die mit Festwertspeichern (ROM) und Schreib-Lese-Speichern (RAM) und mit Speicherplätzen für Prüfinformationen und mit Prüfinformationsgeneratoren ausgerüstet sind und die außerdem Vergleicher enthalten, die die Ausgangsinformation der Zentraleinheiten überprüfen und bei Nicht-Übereinstimmung Abschaltsignale abgeben.

Zu den sicherheitskritischen Regelungssystemen gehören beispielsweise die in die Bremsenfunktion eingreifenden Kraftfahrzeug-Regelungssysteme, von denen insbesondere die Blockierschutzregelungen oder Antiblockiersysteme (ABS) und die Antriebsschlupfregelungssysteme (ASR, TCS, etc.) in vielen Varianten auf dem Markt sind und große Bedeutung besitzen. Fahrstabilitätsregelungssysteme (FSR, ASMS), Fahrwerksregelungssysteme usw. sind ebenfalls sicherheitskritisch, weil sie auf Bremseneingriff beruhen oder weil bei ihrem Versagen auf andere Weise die Fahrstabilität des Fahrzeugs leiden kann. Es ist daher unbedingt erforderlich, die Funktionsfähigkeit solcher Systeme ständig zu überwachen, um beim Auftreten eines Fehlers die Regelung abschalten oder in einen für die Sicherheit weniger gefährlichen Zustand umschalten zu können.

Ein Beispiel für eine Schaltungsanordnung oder ein Microprozessorsystem zur Steuerung und Überwachung einer blockiergeschützten Fahrzeugbremsanlage ist aus der DE 32 34 637 C2 bekannt. Nach dieser Schrift werden die Eingangsdaten zwei identisch programmierten Microcomputern parallel zugeführt und dort synchron verarbeitet. Die Ausgangssignale und Zwischensignale der beiden Microcomputern werden mit Hilfe von redundanten Vergleichern auf Übereinstimmung geprüft. Wenn die Signale voneinander abweichen, wird über eine ebenfalls redundant ausgelegte Schaltung eine Abschaltung der Regelung herbeigeführt. Bei dieser bekannten Schaltung dient einer der beiden Microcomputer zur Erzeugung der Bremsdrucksteuersignale, der andere zur Bildung der Prüfsignale. Bei diesem symmetrisch aufgebauten Microprozessorsystem sind also zwei vollständige Microcomputer, einschließlich der zugehörigen Festwert- und Schreib-Lese-Speicher, erforderlich.

Nach einem anderen bekannten System, nach dem die in der DE 41 37 124 A1 beschriebene Schaltung aufgebaut ist, werden die Eingangsdaten ebenfalls zwei Microcomputern parallel zugeführt, von denen jedoch nur einer die vollständige, aufwendige Signalverarbeitung ausführt. Der zweite Microcomputer dient vornehmlich zur Überwachung, weshalb die Eingangssignale nach Aufbereitung, Bildung von zeitlichen Ableitungen etc. mit Hilfe vereinfachter Regelalgorithmen und vereinfachter Regelphilosophie weiterverarbeitet werden können. Die vereinfachte Datenverarbeitung reicht zur Erzeugung von Signalen aus, die durch Vergleich mit den in dem aufwendigeren Micro-Computer verarbeiteten Signalen Rückschlüsse auf den ordnungsgemäßen Betrieb des Systems zulassen. Durch die Verwendung eines Prüf-Microcomputers geringerer Leistungsfähigkeit läßt sich der Herstellungsaufwand im Vergleich zu einem System mit zwei vollständigen, aufwendigen Microcomputern gleicher Leistung reduzieren.

Ein Microprozessorsystem der eingangs genannten Art ist auch bereits aus der DE 43 41 082 AI bekannt. Es ist insbesondere an die Anwendung für das Regelungssystem einer blockiergeschützten Bremsanlage gedacht. Diese bekannte System, das auf einem einzigen Chip untergebracht werden kann, enthält zwei Zentraleinheiten bzw. CPU's, in denen die Eingangsdaten parallel verarbeitet werden. Die Festwert- und die Schreib-Lese-Speicher, an die beide Zentraleinheiten angeschlossen sind, enthalten zusätzliche Speicherplätze für Prüfinformationen und umfassen jeweils einen Generator zur Erzeugung von Prüfinformationen. Die Ausgangssignale eines der beiden Zentraleinheiten werden zur Erzeugung der Steuersignale weiterverarbeitet, während die andere, die "passive" Zentraleinheit, lediglich zur Überwachung der "aktiven" Zentraleinheit, dient. Durch den Verzicht auf die Verdoppelung der Speicher dieses Systems, unter Inkaufnahme einer relativ geringfügigen Erweiterung der Speicher zur Aufnahme der Prüfinformationen, wird eine erhebliche Verringerung des Herstellungsaufwandes ohne Einbußen an die Fehlererkennbarkeit erreicht.

Der Erfindung liegt ebenfalls die Aufgabe zugrunde, ein Microprozessorsystem so entwickeln, daß mit der äußerst hohen Wahrscheinlichkeit und Zuverlässigkeit, die für sicherheitskritische Anwendungen gefordert wird, Fehlfunktionen des Systems erkennt und signalisiert. Gleichzeitig sollte ein vergleichsweise geringer Herstellungsaufwand für ein solche Microprozessorsystem genügen.

Es hat sich herausgestellt, daß diese Aufgabe mit den im beigefügten Anspruch 1 beschriebenen System gelöst werden kann, dessen Besonderheit darin besteht, daß die Zentraleinheiten bzw. CPU's über separate Bussysteme an die Festwert- und an die Schreib-Lese-Speicher sowie an Eingabe- und an Ausgabeeinheiten angeschlossen sind und daß die Bussysteme untereinander durch Treiberstufen verbunden bzw. gekoppelt sind, die den beiden Zentraleinheiten ein gemeinsamen Lesen und Abarbeiten der anstehenden, d. h. in den beiden Bussystemen zur Verfügung stehenden Daten einschließlich der Prüfdaten und Befehle, ermöglichen. Die auf den beiden Bussystemen anstehenden Eingans- und Ausgangsdaten der beiden Zentraleinheiten, einschließlich der Prüfdaten und Befehle werden von dem oder den Vergleichern des erfindungsgemäßen Systems auf Übereinstimmung überprüft.

In den Unteransprüchen sind noch einige vorteilhafte Ausführungsbeispiele der Erfindung beschrieben.

Das erfindungsgemäße Microprozessorsystem basiert auf der Verwendung von zwei gleichberechtigten, vollredundant betriebenen Rechnerkernen bzw. Zentraleinheiten, die gemeinsam die über zwei separate Bussysteme zugeführten Daten redundant verarbeiten. Mit Hilfe eines einfachen Hardware-Vergleichers, dem aus Sicherheitsgründen ein zweiter Vergleicher parallelgeschaltet ist, werden dann die Eingangs- und die Ausgangssignale beider Zentraleinheiten auf Übereinstimmung verglichen. Die Speicher des erfindungsgemäßen Systems sind nur einmal vorhanden; es sind lediglich zusätzliche Speicherplätze für Prüfdaten, die beispielsweise in Form von Paritätsbits vorliegen, vorgesehen.

Nach einem bevorzugten Ausführungsbeispiel ist an einem der beiden Bussysteme ein vollständiger Microprozessor bestehend aus Zentraleinheit, Festwert- und Schreib-Lese-Speicher, Eingangs- und Ausgangsstufe, angeschlossen, während das zweite Bussystem anstelle

der Festwert- und Schreib-Lese-Speicher nur mit entsprechenden Speicherplätzen für Prüfdaten direkt verbunden ist. Die beide Bussysteme koppelnden Treiberstufen ermöglichen jedoch beiden Zentraleinheiten das Lesen aller benötigten, von den Nutzdaten-Speichern, den Prüfdatenspeichern und den Eingangsstufen gelieferten Daten. Auf diese Weise entsteht eine besonders einfache Struktur des erfindungsgemäßen Microprozessorsystems, die das Unterbringen aller Komponenten auf einem einzigen Chip begünstigt.

Weitere Merkmale, Vorteile und Anwendungsmöglichkeiten gehen aus der folgenden Beschreibung eines Ausführungsbeispiels anhand der beigefügten Abbildung hervor, die in schematisch vereinfachter Darstellung die wichtigsten Komponenten eines Microprozessorsystems nach der Erfindung wiedergibt.

Zur Erläuterung des prinzipiellen Aufbaus und der Wirkungsweise eines Microprozessorsystems nach der Erfindung dient die beigefügte Abbildung. Es handelt sich in diesem Beispiel und ein Ein-Chip-Microcomputersystem, das zwei synchron betriebene Zentraleinheiten 1, 2, die auch als Rechner- oder Prozessorkerne oder als CPU's bezeichnet werden, separate Bussysteme 3, 4 (Bus 1, Bus 2) enthält. Der für beide Zentraleinheiten 1, 2 gemeinsame Takt wird über den Anschluß cl (common clock) zugeführt. Die Zentraleinheit 1 ist durch einen Festwertspeicher 5 (ROM), durch einen Schreib-Lese-Speicher 6 (RAM) und durch Eingabe- oder Eingangsstufen 7, 8 (Peripherie 1, Port 1) und durch eine Ausgabe- oder Ausgangsstufe 9 zu einem vollständigen Microcomputer MC1 ergänzt. An das zweite Bussystem 4 (Bus 2) sind dagegen außer der Zentraleinheit 2 lediglich Prüfdaten-Speicher 10, 11 und außerdem Eingabe- oder Eingangsstufen 12, 13 und eine Ausgabestufe 14 angeschlossen. Die Prüfdaten-Speicherplätze für die Daten im Festspeicher 5 sind in dem Speicher 10, die Prüfdaten für den Schreib-Lese-Speicher 6 im Speicher 11 untergebracht. Das Ganze bildet einen "abgemagerten" Microcomputer MC2.

Die beiden Bussysteme 3, 4 (Bus 1, Bus 2) sind außerdem, was erfindungswesentlich ist, durch Treiberstufen 15, 16, 17 gekoppelt, die es ermöglichen, daß die ankommenden Daten von den beiden Zentraleinheiten 1, 2 gemeinsam gelesen werden können. Die Stufen 15 bis 17 sind Treiber (oder "buffer" mit Enable-Funktion). Die Übertragungsrichtungen der Treiber 15 bis 17 sind durch einen Pfeil symbolisch dargestellt; der Treiber 15 dient zur Übertragung der Daten, die sich auf dem Bussystem 3 (Bus 1) befinden, zur Zentraleinheit 2, der Treiber 16 zur Übertragung der Prüfinformationen oder -daten aus den Prüfdatenspeichern 10, 11 zur Zentraleinheit 1 und der Treiber 17 zur Übertragung der Daten von den Eingangsstufen 12, 13 des zweiten Bussystems 4 (Bus 2) zur Zentraleinheit 1.

Die Bussysteme 3, 4 umfassen jeweils einen Steuerbus "C", einen Datenbus "D" und eine Adress-Bus "A". Auf dem Datenbus befinden sich auch die Prüfdaten "p". Die Eingangs- und die Ausgangsdaten der Zentraleinheiten, die in einem Hardware-Vergleicher 18 und in einem gleichartigen, auf dem gleichen Chip, örtlich getrennt angeordneten Vergleicher 19 auf Übereinstimmung geprüft werden, sind daher in mit "CDpA" bezeichnet.

Im Gegensatz zu bekannten Systemen ist bei dem erfindungsgemäßen Micropozessorsystem keine Unterscheidung in einen aktiven und in einen passiven Rechner möglich. Die beiden Rechnerkerne oder Zentraleinheiten 1, 2 sind vielmehr gleichberechtigt. Sie verarbeiten vollredundant die gemeinsam gelesenen Daten, zu denen auch die Prüf- oder Redundanzinformationen und die Steuerbefehle gehören. Die Eingangs- und die Ausgangssignale der Rechner 1, 2 werden auf Übereinstimmung geprüft und über die zugehörigen Bussysteme 3, 4 und die Ausgabeeinheiten 9, 14 einer symbolisch dargestellten Ventilansteuerung 20 zugeleitet. Diese funktioniert wie folgt:

Beide Zentraleinheiten 1, 2 liefern über die Bussysteme 3, 4 identische Ausgangssignale zu den Ausgabeeinheiten 9, 14. Im Weg zu einer der beiden Ausgabeeinheiten, hier im Weg zur Ausgabeeinheit 14, ist ein Inverter 22 eingefügt. Über einen seriellen Bus 21 ist die Ventilansteuerung 20 angeschlossen. Es sind in diesem Ausführungsbeispiel zwei Ausgangsschieberegister 22, 23 vorgesehen, wobei dem zweiten Schieberegister 22 die Daten invertiert zugeführt werden, um Kurzschlüsse zwischen den Rechnern auszuschließen. Über ein UND-Gatter 24 mit einem invertierenden Eingang werden die in den Schieberegistern 22, 23 enthaltenen Daten auf Übereinstimmung verglichen. Ist die UND-Bedingung, die das Gatter 24 überwacht, nicht erfüllt, wird ein Schalter 26 in der Stromversorgung für die angesteuerten Ventile oder Aktuatoren 25 geöffnet und dadurch, weil ein Fehler vorliegt, die Aktuatorbetätigung abgeschaltet.

Die Schieberegister 22, 23 sind als Bestandteile der Ausgangsstufen 9 bzw. 14 anzusehen. Es wird also unabhängig von den Vergleichern 18, 19 nochmals, in diesem Fall extern, die Übereinstimmung der Ausgangssignale überwacht. Im Fehlerfall wird somit unabhängig von der Funktion der Zentraleinheiten 1, 2 die Ansteuerung der Ventile 25 unterbunden.

Erfindungsgemäß wird also die Zentraleinheit, wozu die Gesamtheit des Rechenwerkes und der Ablaufsteuerung gehört, zur Absicherung der Rechenergebnisse und der richtigen Abarbeitung der Programme doppelt ausgeführt. Der Datenbus wird jeweils um einen Generator für die Prüfdaten bzw. für Redundanzinformation, z. B. für Paritätsbits, erweitert. Die Ausgangssignale der beiden Zentraleinheiten, werden zur Überprüfung an die Hardware-Vergleicher (18, 19) geleitet. Diese überprüfen die Identität der Signale, einschließlich der Prüfsignale, und bewirken eine System-ABSCHALTUNG, wenn die synchrone Abarbeitung der Programme durch die redundanten Zentraleinheiten voneinander abweichende Resultate ergeben.

Die Ausgangssignale beider Zentraleinheiten sind gleichberechtigt, d. h. eine Ansteuerung von Speichereinheiten (RAM, ROM) oder der "Peripherie" kann durch eine der beiden Zentraleinheiten erfolgen.

Über die Eingabeeinheiten 7, 12, die in der Abbildung als Peripherie 1 und Peripherie 2 bezeichnet sind, können bei einem Kraftfahrzeugregelungssystem z. B. die Radsensoren, deren Ausgangssignale die wichtigsten Eingangsgrößen des Regelungssystems sind, angeschlossen werden. Dabei ist es möglich, die Sensorsignal-Zuführung wie dargestellt, auf die beiden Bussysteme 3, 4 zu verteilen. Die Signalzuführung kann natürlich auch redundant, nämlich durch Anschluß aller Sensorsignale an beide Bussysteme 3, 4, ausgebildet werden.

Entsprechendes gilt für die über die Eingabestufen 8, 13 (Port 1, Port 2) zugeführten Informationen. Bei einem geregelten Bremsensystem werden über diese Eingabestufen beispielsweise der Bremslichtschalter und andere Sensoren angeschlossen.

Ein wichtiges Merkmal der Erfindung ist darin zu sehen, daß — trotz der weitgehenden Redundanz und "Absicherung" des Datenverarbeitungsprozesses — der

Speicheraufwand relativ klein gehalten wird. Die Festwert- und die Schreib-Lese-Speicher sind nämlich, wie zuv r erläutert, lediglich für einen der beiden Microcomputer (MC1) vorgesehen, während an den zweiten Micr computer (MC2) lediglich Speicherplätze (10, 11) für Prüfdaten besitzt. Die Treiberstufen 15, 16, 17 mit denen beid Bussysteme gekoppelt sind, stellen sicher, daß dennoch im Datenverarbeitungsprozeß beiden Zentraleinheiten die gespeicherten Nutzdaten und Prüfdaten zur Verfügung stehen.

Abweichend von dem dargestellten Ausführungsbeispiel können die Speicherplätze der Speicher 5, 6, 10, 11 auch völlig anders auf die beiden Bussysteme 3, 4 bzw. Microcomputer MC1, MC2 verteilt werden. Der insgesamt erforderliche Speicherplatz wird dadurch nicht erhöht.

Zur Fehlererkennung beim Lesen und Schreiben der gespeicherten und abzuspeichernden Daten werden die Prüfdaten bzw. Paritätsbits herangezogen. Zu jeder Speicherzelle des Festwert- und des Schreib-Lese-Speichers ist unter der gleichen Adresse in den Speichern 10, 11 des zweiten Microprozessors MC2, der nur Speicherplätze für die Prüfdaten enthält, die Redundanzinformation abgelegt. Für den Festwertspeicher wurde die Prüf- bzw. Redundanzinformation bereits während der Programmierung festgelegt. Bei den Schreib-Lese-Speichern wird diese Prüf- bzw. Redundanzinformation beim Schreibvorgang generiert. Analog zu dem Lesevorgang der Daten und Befehle wird die Prüf- bzw. Redundanzinformation über die Treiberstufe 16, die die beiden Bussysteme 3, 4 koppelt, übertragen. Beim schreibenden Zugriff werden demnach die zu schreibenden Daten um eine redundante Information erweitert, die mit den Daten gespeichert werden. Bei einem lesenden Zugriff werden diese Daten und die zurückgelesene redundante Information dann durch die Vergleicher 18, 19 auf Gültigkeit überprüft.

Sollen aus Sicherheitsgründen Eingangsdaten redundant erfaßt und verarbeitet werden, werden die Eingangs- bzw. Eingabestufen (7, 8, 12, 13) doppelt ausgelegt. Diese Stufen können jeweils zum Teil im Adreßraum der einen und der anderen Zentraleinheit angeordnet werden. Daher ist eine Entkopplung der Peripherie-Elemente wie bei einem symmetrischen Microprozessorsystem gegeben.

Die Ausgangssignale, insbesondere die Ansteuersignale für die Ventilansteuerung 20, die doppelt ausgelegte Ausgabestufen enthalten, können ebenfalls jeweils zum Teil im Adreßraum der einen oder der anderen Zentraleinheit angeordnet werden. Folglich ist eine Entkopplung von Ausgangs-Peripherie-Elementen wie bei einem vollsymmetrischen Konzept gegeben.

Um Fehler bei der Übertragung von Informationen über das Bussystem zu erkennen, ist dieses redundant in Form der Bussysteme 3 und 4 (Bus 1, Bus 4) ausgelegt. Die von den beiden Zentraleinheiten 1, 2 abgegebenen, auf den Bussystemen anstehenden Signale werden durch die Vergleicher 18, 19 auf Übereinstimmung überwacht.

Werden zur Erzeugung der Prüfdaten oder Redundanzdaten Paritätsgeneratoren verwendet, sind bei dem erfindungsgemäßen System zwei Generatoren erforderlich, die z. B. in den Zentraleinheiten 1, 2 oder in den Vergleichern 18, 19 untergebracht werden können. Bei einem schreibenden Zugriff auf die zusätzlichen Speicherplätze, die für den Schreib-Lese-Speicher zur Verfügung stehen (Speicher 11), wird die mit Hilfe des Redundanzgenerators in der Zentraleinheit 2 erzeugte Information gespeichert. Bei lesendem Zugriff auf die zusätzlichen Speicherplätze für die Prüfdaten im Festwert- oder Schreib-Lese-Speicher wird die von dem Redundanzgenerator erzeugte Information mit der gelesenen Redundanzinformation auf Übereinstimmung verglichen.

Geeignete Redundanzgeneratoren lassen sich z. B. in bekannter Weise mit Hilfe von Exklusiv-ODER-Gattern realisieren.

Patentansprüche

1. Microprozessorsystem für sicherheitskritische Regelungen, mit zwei synchron betriebenen Zentraleinheiten oder CPU's, die die gleichen Eingangsinformationen erhalten und das gleiche Programm abarbeiten, mit Festwertspeichern (ROM) und Schreib-Lese-Speichern (RAM), mit Speicherplätzen für Prüfdaten und mit Prüfdatengeneratoren, mit Vergleichern, die die Ausgangsdaten bzw. Ausgangssignale der Zentraleinheiten überprüfen und bei Nicht-Übereinstimmung Abschaltsignale abgeben, **dadurch gekennzeichnet,** daß die Zentraleinheiten bzw. CPU's (1, 2) über separate Bussysteme (3, 4) an die Festwert- und an die Schreib-Lese-Speicher (5, 6, 10, 11) sowie an Eingabe- und Ausgabeeinheiten (7, 8, 12, 13; 9, 14) angeschlossen sind und daß die Bussysteme (3, 4) untereinander durch Treiberstufen (15, 16, 17) verbunden sind, die den beiden Zentraleinheiten (1, 2) ein gemeinsames Lesen und Abarbeiten der anstehenden, d. h. in den beiden Bussystemen (3, 4) zur Verfügung stehenden Daten, einschließlich der Prüfdaten und Befehle, ermöglichen.

2. Microprozessorsystem nach Anspruch 1, dadurch gekennzeichnet, daß die Vergleicher (18, 19) die auf den beiden Bussystemen (3, 4) anstehenden Eingangs- und Ausgangsdaten der beiden Zentraleinheiten (1, 2), einschließlich der Prüfdaten und Befehle auf Übereinstimmung vergleichen.

3. Microprozessorsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Speicherplätze der Festwertspeicher (5) und der Schreib-Lese-Speicher (6), einschließlich der Speicherplätze für die Prüfdaten (10, 11), auf die an die beiden Bussysteme (3, 4) angeschlossenen Speicher (5, 6, 10, 11) verteilt sind.

4. Microprozessorsystem nach Anspruch 3, dadurch gekennzeichnet, daß an einem Bussystem (3) die Festwert- und die Schreib-Lese-Speicher (5, 6) und an dem zweiten Bussystem (4) die zugehörigen Prüfwertspeicher (10, 11) angeschlossen sind.

5. Microprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zumindest die beiden Zentraleinheiten (1, 2), die Speicher (5, 6, 10, 11) und die Treiberstufen (15, 16, 17), die den Zentraleinheiten ein gemeinsames Lesen der anstehenden Daten ermöglichen, und ein Vergleicher (18, 19) auf einem einzigen Chip angeordnet sind.

6. Microprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die beiden Bussysteme (3, 4) jeweils einen Daten- und Prüfinformations-Bus (Dp), einen Adreßbus (A) und einen Steuerbus (C) umfassen.

7. Microprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Signale der beiden Zentraleinheiten (1, 2),

nämlich die Signale auf den beiden Bussystemen (3, 4), zwei parallel geschalteten Hardware-Vergleichern (18, 19) zugeführt werden, die innerhalb eines Chips, jedoch räumlich getrennt, angeordnet sind.

8. Microprozessorsystem nach einem oder mehreren der Ansprüchen 1 bis 7, dadurch gekennzeichnet, daß an die Systeme (3, 4) mit einem externen Vergleicher (22, 23, 24) Aktuatoren oder Ventile angeschlossen sind.

9. Microprozessorsystem nach Anspruch 8, dadurch gekennzeichnet, daß der externe Vergleicher (2) Ausgangsschieberegister (22, 23) aufweist, von denen eines (23) die Ausgangsdaten invertiert erhält, daß die den beiden Schieberegister (22, 23) enthaltenen Daten über ein UND-Gatter (24), das einen invertierten Eingang besitzt, verglichen werden und daß das Ausgangssignal des UNDF-Gatters (24) einen Schalter (26) in der Stromversorgung für die Aktuatoren oder Ventile (25) geschlossen hält.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 195 29 434 A1
Int. Cl.[6]: G 05 B 9/03
Off nlegungstag: 13. Februar 1997